ABSTRACT OF THE DISCLOSURE

A method for certifying public keys of a digital signature scheme in a communications system is provided. The secure communications system is one in which there are at least two levels of authorities. A user presents a piece of data to an intermediate level authority who, upon verifying the data, causes an issuing authority to issue a certificate that the piece of data posses a given property. Although the certificate is compacted by not having it contain a pubic key of the intermediate authority, nonetheless, information is stored in order to keep the intermediate authority accountable.